CV and Research Statement

Markus Jakobsson
www.linkedin.com/in/markusjakobsson
www.markus-jakobsson.com

1 At a Glance

- **Focus.** *Identification of security problems, trends and solution along four axes –* computational*,* structural*,* physical *and* social*; quantitative and qualitative fraud analysis; development of disruptive security technologies.*

- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1994).

- **Large research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); PayPal (Principal Scientist of Consumer Security, Director, 2010-2013); Qualcomm (Senior Director, 2013-2015); Agari (Chief Scientist, 2016–2018); Amber Solutions Inc (Chief of Security and Data Analytics, 2018 – current)

- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2016).

- **Entrepreneurial activity.** *ZapFraud* (Anti-scam technology; CTO and founder, 2012-); *RavenWhite Security* (Authentication solutions; CTO and founder, 2005-); *RightQuestion* (Consulting; Founder, 2007-); *FatSkunk* (Malware detection; CTO and founder, 2009-2013 – FatSkunk was acquired by Qualcomm); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2013); *CellFony* (Mobile security; Member of technical advisory board, 2009-2013); *PopGiro* (User Reputation; Member of technical advisory board, 2012-2013); *MobiSocial* (Social networking, Member of technical advisory board, 2013); *Stealth Security* (Anti-fraud, Member of technical advisory board, 2013–current)

- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2011); *Boku* (2009-2010); *Western Union* (2009-2010).

- **Intellectual Property, Testifying Expert Witness.** *Inventor of 100+ patents; expert witness in several patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale; Hunton & Williams; Quinn Emanuel Urquhart & Sullivan; Freed & Weiss; Berry & Domer; Fish & Richardson; DLA Piper; Cipher Law Group; Keker & Van Nest). Details and references upon request.
- **Publications**. Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crimeware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *The Death of the Internet* (Wiley, 2012); *Towards Trustworthy Elections: New Directions in Electronic Voting* (Springer Verlag, 2010); *Understanding Social Engineering* (Springer Verlag, 2016); *100+ peer-reviewed publications*

2 Summary

I am one of the more prominent computer scientists studying fraud and fraud prevention. I have performed and published novel research on fraud and authentication since 1993, with a focus on the payments industry since 1995. In 1999, I posited that what later became known as phishing would become a big problem. As a Principal Scientist at RSA Laboratories in 2001, my mandate was to determine the impact of future fraud scenarios on commerce and authentication, and developing intellectual property to address such problems. In 2004, I built a research group around online fraud and countermeasures, resulting in more than 50 publications and two books ("Phishing and Countermeasures", Wiley; "Crimeware", Symantec Press.) I co-founded the first company to address consumer security education, and am a pioneer in that area. I also co-founded an RSA Security spinoff (RavenWhite Security), and a company to address mobile malware (FatSkunk), and have overseen their intellectual property creation. FatSkunk was acquired by Qualcomm in 2013. I also founded ZapFraud, a company addressing Business Email Compromise. I am currently the Chief Scientist at Agari, a company addressing email-based fraud.

I have recruited and supervised junior colleagues, developers and PhD/Masters students for fifteen years. I have been in charge with building research groups at Bell Laboratories, RSA Laboratories and Indiana University. I was the most senior security researcher at Indiana University, and was hired to Xerox PARC to provide thought leadership to their security group. My former advisees have prominent roles at RSA Laboratories, Mozilla, Google, and top universities such as MIT and ETH Zurich MIT. I played a prominent role in defining the intellectual property efforts at PayPal/eBay, and contributed significantly to their portfolio. I founded and built FatSkunk, bringing a new security paradigm to the marketplace.

3 Recent Focus

My work primarily involves identifying trends in fraud and computing before they affect the market, and to develop and test countermeasures – whether technical, or based on user interaction or education. I am the inventor of more than 100 patents. At PayPal, I developed and tested a technology that allows the automatic creation of PINs from passwords [46], with direct applications to improved mobile security and simplified user experience. I also studied liar buyer fraud [39] and developed improved authentication and fraud detection methods. At FatSkunk, I developed a new Anti-Virus paradigm (see, e.g., [42]); protected the intellectual property; built a team to build the technology; and worked towards commercializing the technology. After the acquisition of FatSkunk, this work was continued at Qualcomm, where I also worked on IoT, wearable authentication methods [41], anti-theft technology and privacy technology aimed at automatically detecting and block attempts to track users. My work at ZapFraud focused on understanding and blocking email scams [40], with a focus on business email compromise, and building a foundational patent portfolio. My work at Agari addressed enterprise-facing scams such as Business Email Compromise, Ransomware, and other abuse based on social engineering and identity deception. My work at Amber Solutions involve protocol design for defending against attacks on consumer and enterprise sensor networks.

My PhD is in theoretical computer science, but my later emphasis has been on applied security, including authentication, click-fraud [29], mobile malware detection [42], detection of business email compromise, and the development of metrics to detect new types of fraud.

4 My Beliefs

Security research is commonly carried out from a perspective that is not cross-disciplinary, and which only takes into consideration a portion of the issues affecting the security of the system. This creates results that bring to mind the story of the blind men and the elephant – showing that without a holistic view of a system, it is easy to misunderstand it. Dramatic progress can sometimes only be made by understanding a problem in a holistic manner.

The security of a system can be described along (at least) three dimensions:

One dimension of relevance is the typical behavior of the end user. A first example of this is the context of phishing: It is largely meaningless to design phishing countermeasures without first understanding end-user psychology, including how typical users react both to fraud and to potential fraud countermeasures. I studied phishing before it was an academic discipline; built an understanding of how typical users react to common security measures (such as Bank of America's SiteKey, which provides only negligible security); and I created methods to heuristically measure the success of security solutions that were designed with typical user behavior in mind. A second example of the importance of understanding end-user behavior involves how people create passwords; how traditional password strength meters fail to measure strength in any meaningful manner; and how to design password strength meters that work, informed by an understanding of how people create passwords. These two examples demonstrate how an understanding of end-user behavior can guide protocol design and user interface design (as in the first example) and back-end risk assessments (as in the second example.)

A second dimension of relevance in the context of the design of security measures is an understanding of the typical adversary. As a first example, in my research on so-called Nigerian scams, I have studied adversarial behavior, including copycat behavior and adaptive behavior. Based on the insights from this work, I developed novel natural language processing techniques and associated spam filters that exhibit dramatically lower error rates than traditional spam filters. This effort was both guided by current adversarial behavior, and by an understanding of possible adversarial changes and likely reactions to deployed security measures. A second example underlining the importance of understanding adversarial behaviors – including where traditional security measures are likely to drive adversarial behavior – is my work on mobile malware detection.

My work on mobile malware detection also shows the importance of understanding the third dimension: understanding computational limitations and hardware constraints; algorithmic limitations; and deployment constraints. My work in this area shows how being able to understand computational constraints and hardware constraints enables new and dramatically improved security paradigms to be developed. The FatSkunk technology is just one example of this opportunity.

Even security problems that at first sight appear to many to be one dimensional commonly turn out to have two or more dimensions. Mobile security mechanisms, for example, need to recognize the potential impact of the different use of these platforms in comparison with traditional computers. A concrete example of this is the impact of screen size on security via reduced abilities to convey security information: Mobile browsers allow websites to cause the address bar to be scrolled off the screen, which has a direct impact on the ability of users to make security decisions based on inspecting the URL of a visited site. Another concrete example relates to "liar buyer fraud". Estimated to account for about a third of PayPal's fraud losses, it is a problem that has defied traditional anti-fraud technologies. Using a simple change in what information is displayed to a user – whether honest or not – offers a promise to dramatically reduce the losses arising from this type of fraud [39].

My research. One can define an adversarial opportunity as the possibility for an adversary to increase his or her yield, where the yield can loosely be defined as the profit at a particular risk and effort. It is possible to estimate adversarial opportunities. Simply speaking, there is a great adversarial opportunity when there exists scams (whether currently used or not) that current security solutions do a poor job addressing, seen in the light of typical user behavior. I identify areas with big adversarial opportunity by building an understanding of systemic weaknesses and psychological vulnerabilities. Here, the establishment of an understanding of the adversarial opportunity depends on an understanding of the three dimensions of the associated problem.

Given an area associated with a great adversarial opportunity, the next step is to find ways to reduce the size of this opportunity, or, stated more simply, to design improved security solutions. This task, just like the task of assessing adversarial opportunity, is informed by an understanding of the three dimensions associated with the problem, seen in the light of each potential individual security measure. Given areas of great adversarial opportunity, I identiy security solutions that appear to reduce this opportunity the most. I then construct ways to provide assurance of this reduction – whether experimentally or using analytical or deductive methods.

As soon as I succeed in identifying promising solutions to vexing problems, I address the intellectual property aspect, which is a fourth dimension associated with a problem. This is an area I am passionate about. I am named as inventor on more than seventy issued patents, and at least as many pending. I commonly draft claims, and am always involved in addressing office actions. In addition, I have served as testifying expert witness in an array of patent litigation cases stretching from digital rights management and hardware-based security to mobile security and secure messaging, further feeding my awareness of what makes a patent strong – or not so strong.

Vision of future needs. It is not meaningful to try to defend against a threat that one does not understand. The first step must be to understand and quantify the problem, and to recognize what constrains the possible solutions. This must be done in terms of the *computational*, *structural*, *physical* and *social* dimensions.

There is a substantial need for work that secures the infrastructure, whether from technical or social threats. This will involve malware detection and recovery; robustness against denial of service and denigration attacks; establishment of identity (whether device or user); maintenance of trust (on both a technical and human level); user communication (including avoidance of social engineering, how to communicate important information to unmotivated users, and how to build security mechanisms that are usable in the face of adversarial campaigns). There is also need to recover from failures on various levels; and to use anomaly detection for early-warning systems. It is important to understand that user behavior will change dramatically in situations of attack, and this may in itself destabilize systems. To address these issues, a broad understanding of vulnerabilities, technologies, and trends is necessary.

5 Publication List

Books (1-6); book chapters, journals, conference publications and other scientific publications (7-147), issued /published U.S. patents (148-234). For an updated list, and for international patents, please see `www.markus-jakobsson.com/publications` and appropriate patent search engines.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.